ABSTRACT OF THE DISCLOSURE

This invention provides a method for accelerating multiplication of an elliptic curve point Q(x,y) by a scalar k, the method comprising the steps of selecting an elliptic curve over a finite field Fq where q is a prime power such that there exists an endomorphism Ψ, where $\Psi(Q)=\lambda.Q$ for all points Q(x,y) on the elliptic curve: and using smaller representations k_i of the scalar k in combination with the mapping Ψ to compute the scalar multiple of the elliptic curve point Q.